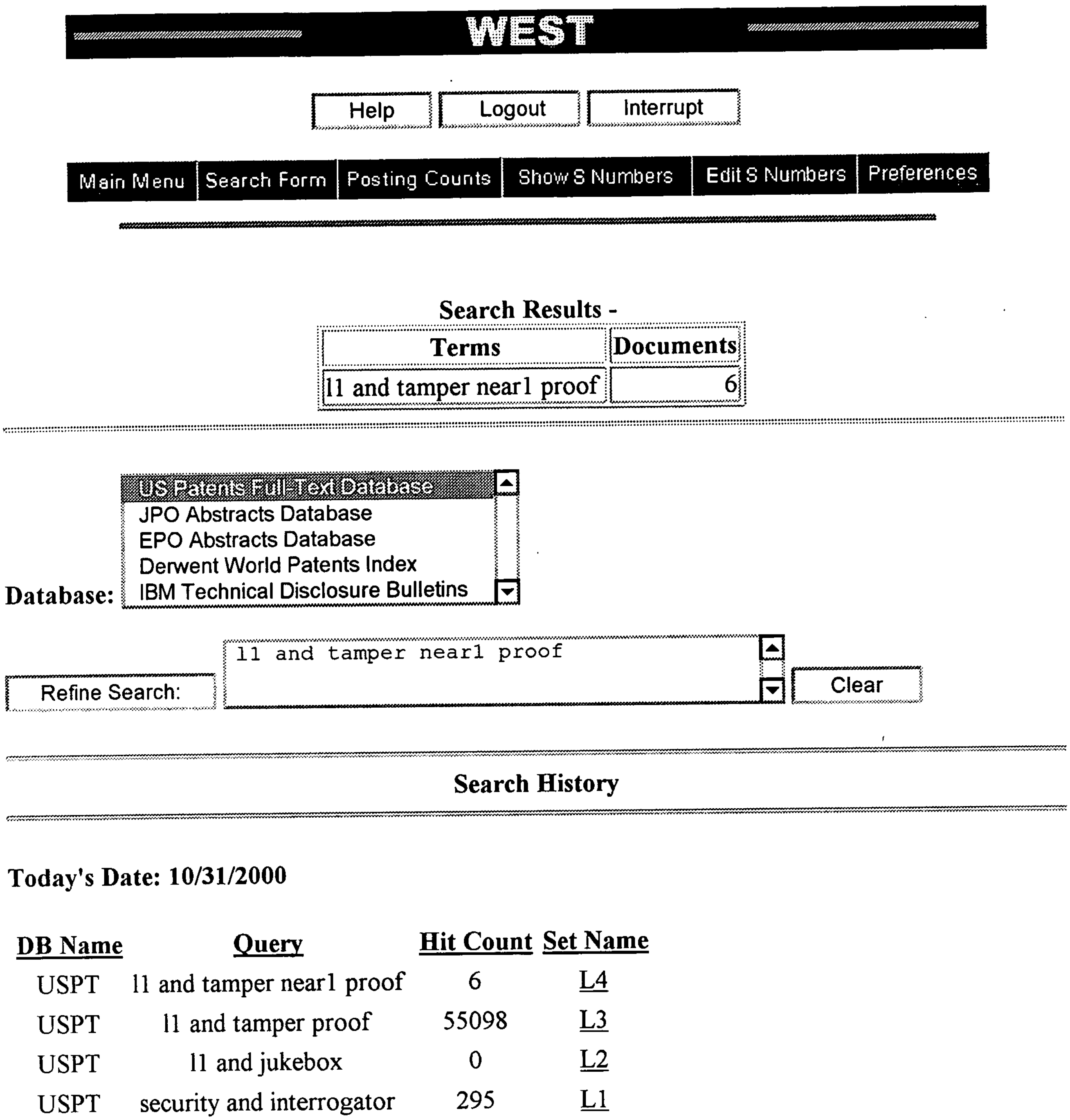

Search Results -

Terms	Documents
l1 and tamper near1 proof	6

Database:
- US Patents Full-Text Database
- JPO Abstracts Database
- EPO Abstracts Database
- Derwent World Patents Index
- IBM Technical Disclosure Bulletins

Refine Search: l1 and tamper near1 proof

Search History

Today's Date: 10/31/2000

DB Name	Query	Hit Count	Set Name
USPT	l1 and tamper near1 proof	6	L4
USPT	l1 and tamper proof	55098	L3
USPT	l1 and jukebox	0	L2
USPT	security and interrogator	295	L1

WEST

Generate Collection

Search Results - Record(s) 1 through 6 of 6 returned.

□ 1. Document ID: US 5892454 A

L4: Entry 1 of 6 File: USPT Apr 6, 1999

US-PAT-NO: 5892454
DOCUMENT-IDENTIFIER: US 5892454 A
TITLE: Hybrid monitoring of location of a site confinee

Full | Title | Citation | Front | Review | Classification | Date | Reference | Claims | KWIC | Draw Desc | Image

□ 2. Document ID: US 5568119 A

L4: Entry 2 of 6 File: USPT Oct 22, 1996

US-PAT-NO: 5568119
DOCUMENT-IDENTIFIER: US 5568119 A
TITLE: Arrestee monitoring with variable site boundaries

Full | Title | Citation | Front | Review | Classification | Date | Reference | Claims | KWIC | Draw Desc | Image

□ 3. Document ID: US 5485520 A

L4: Entry 3 of 6 File: USPT Jan 16, 1996

US-PAT-NO: 5485520
DOCUMENT-IDENTIFIER: US 5485520 A
TITLE: Automatic real-time highway toll collection from moving vehicles

Full | Title | Citation | Front | Review | Classification | Date | Reference | Claims | KWIC | Draw Desc | Image

□ 4. Document ID: US 5469363 A

L4: Entry 4 of 6 File: USPT Nov 21, 1995

US-PAT-NO: 5469363
DOCUMENT-IDENTIFIER: US 5469363 A
TITLE: Electronic tag with source certification capability

Full | Title | Citation | Front | Review | Classification | Date | Reference | Claims | KWIC | Draw. Desc | Image

---

□ 5. Document ID: US 5430447 A

```
L4: Entry 5 of 6          File: USPT          Jul 4, 1995

US-PAT-NO: 5430447
DOCUMENT-IDENTIFIER: US 5430447 A
TITLE: Protection against manipulation of batteryless
read/write transponders
```

Full | Title | Citation | Front | Review | Classification | Date | Reference | Claims | KWIC | Draw. Desc | Image

---

□ 6. Document ID: US 3697984 A

```
L4: Entry 6 of 6          File: USPT          Oct 10, 1972

US-PAT-NO: 3697984
DOCUMENT-IDENTIFIER: US 3697984 A
TITLE: COMPUTER-ALARM INTERFACE SYSTEM
```

Full | Title | Citation | Front | Review | Classification | Date | Reference | Claims | KWIC | Draw. Desc | Image

---

Generate Collection

Terms	Documents
l1 and tamper near1 proof	6

Display | 10 | Documents, starting with Document: | 6

Display Format: | TI | Change Format

WEST

Generate Collection

Search Results - Record(s) 1 through 1 of 1 returned.

□ 1. Document ID: US 5706457 A

```
L2: Entry 1 of 1          File: USPT               Jan 6, 1998

US-PAT-NO: 5706457
DOCUMENT-IDENTIFIER: US 5706457 A
TITLE: Image display and archiving system and method
```

Full | Title | Citation | Front | Review | Classification | Date | Reference | Claims | KWIC | Draw Desc | Image

Generate Collection

Terms	Documents
l1 and digital near1 imag$3	1

Display 10 Documents, starting with Document: 1

Display Format: TI Change Format

WEST

□ Generate Collection

L4: Entry 4 of 6 File: USPT Nov 21, 1995

DOCUMENT-IDENTIFIER: US 5469363 A
TITLE: Electronic tag with source certification capability

ABPL:
An inventory control system uses an electronic tag that keeps an unalterable log of each step in the handling of a controlled item, which may be a flight safety critical aircraft replacement part. The tag is electrically powered via an inductive coupling to a computer with which it communicates, and comprises a non-volatile computer memory element configured so that data may be written into unused portions of it, but so that no existing data can be overwritten or erased. Each tag contains an unalterable secret identification record that is only accessible to a user who has a valid password. As a countermeasure against sophisticated theft attempts involving communicating with the "smart tag" to defeat the security system by learning the password and thereafter altering identification records, etc., the tag permits only a limited number of attempts to read out the secret identification number.

BSPR:
U.S. Pat. No. 5,168,263 to Drucker et al, who teach the use of a "smart tag" containing a tag microprocessor that communicates with other security apparatus via a radio-frequency link; and

BSPR:
The EAS art includes a variety of methods of dealing with thieves who might try either to remove a tag prior to stealing merchandise or to shield the tag on an article of merchandise from detection apparatus located at the exit to a store. The tag art does not extend to providing countermeasures against sophisticated theft attempts involving communicating with a "smart tag" in order to defeat the security system by altering identification records or other data stored in the tag.

BSPR:
Although a variety of measurements, data storage and retrieval methods have been provided by "smart tracer" datalogging devices, these devices are generally used in situations where data security is of little concern. This art area does not provide teaching of a data storage element resistant to sophisticated tampering.

DEPR:
Turning now to FIG. 1 of the drawing, one finds a schematic

block diagram of a tag 10 of the invention. The preferred tag 10 has no battery or other internal source of electrical power, and is expected to have a shelf life at least as long as the shelf life of a protected article. The tag 10 is powered via an inductive coupling circuit 12 that is also used for communication between the tag 10 and the balance of the security system, as has been taught, inter alia by Vinding in U.S. Pat. No. 3,299,424. The inductive coupling circuit 12 includes an antenna coil 14 and a capacitor 16 constituting a tuned circuit 18 that is preferably tuned to resonate at a frequency of about twenty seven megahertz. Electrical power received by the tuned circuit 18 is rectified (e.g., by a Schottky diode 20) and smoothed by a resistor-capacitor pair 22. (The RC time constant of the resistor-capacitor pair 22 is selected to be the minimum needed to adequately smooth the rectified DC output of the Schottky diode 20, and is constrained to be small enough that it does not also obliterate data pulses). Smoothed and rectified DC current passes through a blocking diode 24 and thence into a regulator 26 that has the circuit supply voltage, V.sub.CC, as its output 27. Some of the charge passing through the blocking diode 24 is stored on a large capacitor 28 that powers the circuit during part of the communication process, as will be subsequently described.

DEPR:
Data are preferably downloaded from an interrogator 30 (shown in FIG. 3) to the tag 10 by momentarily turning off the RF power supplied by the interrogator 30, which causes a receiver-controlling field effect transistor 32 to turn off. This, in turn, causes logic circuits in the data receiver 34 to respond to serial data in a manner well known in the art. Data are uploaded from the tag 10 to the interrogator 30 via a transmitter field effect transistor 36 that is momentarily turned on by the data transmitter 38 for each zero in a serial message. During the intervals that the transmitter FET 36 is ON, energy stored on the storage capacitor 28 maintains an adequate input voltage on the voltage regulator 26.

DEPR:
Data from the operation of the tag 10 are stored in an EEPROM 44, which is a standard component and may be a National Semiconductor Corporation NMC93C66, which has a capacity of five hundred and twelve bytes. The EEPROM 44 is preferably a separate component (e.g., with a housing indicated in phantom as 45) that can be mounted with the microprocessor circuitry 46, the storage capacitor 28, the inductive coupling circuit 12, and a one-time actuable circuit element 48 on a circuit board 50. After the tag circuitry 52 is tested, a logical input 54 to the microprocessor 40 is toggled to clear the EEPROM 44, and the tag circuitry 52 is potted or sealed into a tamper-proof enclosure 56 to complete the manufacturing process. Once the tag 10 is sealed, the inductive coupling circuit 12 is the only means by which data can be loaded into or read from it.

DEPR:
Turning now to FIG. 3 of the drawing, one finds a schematic

block diagram of a interrogator 30, which may be configured as the illustrated combination of a battery-powered portable interface unit 80 and a handheld wand 82 connected with a shielded cable 86. in the interest of providing a simpler presentation the battery and power supply circuitry in the interface unit 80 are not shown in the view of FIG. 3. It will be understood to those skilled in the art that the packaging arrangement shown in FIG. 3 is one expected to be convenient for a large number of users, but that other configurations may well be employed.

DEPR:
The data interface unit 80 preferably serves as an interface between the tag 10 and a local computer 104, which may be any of a number of such machines, but which is expected to be one of the many "IBM PC-compatible" machines built around an Intel 80386, or similar, microprocessor. Data entered into or stored in the local computer 104 are downloaded in a half duplex mode into the tag 10 via a conventional serial port 106, which is connected to a corresponding serial port 108 on the data interface unit 80. A RS232 receiver circuit 110 in the data interface unit 80 causes the solid state relay 92 to open whenever a zero is to be sent to the tag 10. As previously noted herein, data are uploaded from the tag 10 to the interrogator 30 via a transmitter field effect transistor 36 that is momentarily turned on by the data transmitter 38 for each zero in a serial message. When the transmitter FET 36 turns on, this causes a drop in the voltage at the output to the power limiting resistor 94, which is demodulated by an amplitude detector circuit 112 that incorporates well known automatic gain control and binary decision threshold capabilities. The output of the detector 112 is amplified by another circuit 114 to standard serial interface levels that are supplied via the serial ports 108, 106 to the local computer 104.

DEPR:
The part-tracking method offered by the apparatus of the invention depends on the use of the EEPROM 44 to record data on successive events as the protected part moves through a distribution system, and to maintain a covert identification and tracking code specific to that part. This process may preferably involve the use of two different security encoding levels, and is best supplied by an EEPROM 44 memory segmented as shown in FIG. 4 of the drawing. An initial block 120 in the EEPROM 44 is written when the tag 10 is originally assigned to an item to be tracked. The initial block 120 may include a manufacturer's valid password 122; a secret identification record 124 that is uniquely associated with a specific chosen item and that will be called the secret identification number (since it has some of the functional attributes of a serial number, even though it is not a simple sequentially assigned number); an overt manufacturer's item identification record 126; and a telephone number 128 assigned to the manufacturer of the protected item. The initial block always includes at least one record (hereinafter called the lock byte 130) that is set when the EEPROM 44 is initially written, thus beginning a

secure mode of operation for the tag 10. As will subsequently be discussed with respect to FIG. 5 of the drawing, the microprocessor 40 reads the lock byte 130 when it is powered up. If the lock byte 130 is set, the microprocessor 40 may write data to unused portions of the EEPROM 44, but will neither erase nor overwrite those portions of the EEPROM memory 44 that already contain data. The sole exception to this rule involves an access attempt number record 132, or byte, that contains a current record of the number of times a given tag 10 has been interrogated. The access attempt byte 132, which may be conveniently set to hold the number "1" at the time of initiation, is usually incremented and overwritten with a new datum each time a request to read the secret identification code is made.

DEPR:
If the microprocessor finds the lock byte 130 is set in Step 146 the program follows the normal operating path by uploading the unprotected data (Step 152), and then waiting for either a further upload request or an additional command (Step 154). If a test password is received it is checked to see if it is the same as the valid password (Step 156). If the two passwords match, the number of accesses is incremented (Step 158) and checked (Step 160) to see if the current number of accesses exceeds a preset limit. If a maximum value assigned to the number of allowable accesses has been exceeded, the program enters a "do nothing" branch by returning control to Step 154, following which only the unprotected data are available from the tag. If, on the other hand, the number of accesses is within preset limits, the certificate number and the manufacturer's phone number are uploaded to the interrogator (Step 162).

CLPR:
9. Apparatus of claim 6 wherein said means of receiving electric power and said means for communicating data comprise an inductive coupling between a said tag and a said interrogator.

CLPR:
10. The tracking system of claim 6 wherein the means for receiving power from the interrogator power supply comprises the sole means of powering the tag.

CLPV:
a plurality of interrogation stations, each said interrogation station comprising a computer controlling an interrogator, said interrogator comprising power supply and interface means, each said computer further comprising an interrogation station memory containing as a record therein a unique interrogation station identification record;

CLPV:
a interrogation station acting under operator control to communicate to said tag microprocessor ones of: a said trace record, each said trace record containing an interrogator identification record: a data upload request; and a test

password;

CLPW:
means for receiving power from said interrogator power supply,

CLPW:
tag communication means transmitting data to and receiving data from said interrogator interface means, and